QuickChick: A Coq Framework For Verified Property Based Testing

Zoe Paraskevopoulou

September 8, 2014
Overview

- **Goal**: Trust high-level logical propositions instead of executable testing code
  - Gain confidence that the right conjecture is being tested
  - Gain confidence that the testing is thorough

- **Means**: Automatically map executable testing code *(checkers)* to logical propositions
  - Reasoning about probabilistic programs *(generators)*
    - map them to sets of outcomes

- **Evaluation**: Application to a number of sizable case studies
  - Modularity
  - Scalability
  - Minimal changes to existing code
Property-Based Testing

- Popularized by QuickCheck in the FP community
- Achieves a high level of automation
  - Randomly Generated Data
    - No need to maintain test suites
  - The programs are being tested against specifications
    - No need for human oracle
- The user has to write
  - Generators
    - Fine-tuning
    - Generation of used defined data types
  - Checkers
    - Programs that test the desired specification
QuickChick

- Randomized property-based testing framework for Coq
  - More precisely a port of QuickCheck in Coq
- Checkers need to be executable
  - No way to directly refute proof goals
- Written in Gallina
- Uses extraction to OCaml for:
  - Acquiring random seeds
  - Efficient execution
  - Generation of numeric (nat and Z) and boolean values
The value of counterexamples

• QuickChick returns counterexamples for falsifiable conjectures
  ♦ Support for shrinking
    ▶ try to isolate the part of the failing input that triggers the failure

• A counterexample could indicate:
  ♦ errors in program
    ▶ fix bug
  ♦ errors in specifications
    ▶ reformulate checker

• Valuable feedback to understand and fix errors
But ... 

How much confidence can we have about the program under test adhering its specifications, when the testing cannot find any more bugs?
Reasons for inadequate testing

Bugs in generators

• May fail to cover sufficiently the input space
  ♦ Some counterexamples may never generated
• May fail to satisfy preconditions of conditional specifications
  ♦ A big portion of the generated data can be discarded

Bugs in checkers

• May fail to capture the desired specifications
  ♦ Too strong preconditions, faulty definitions, . . .
VeriQuickChick

Idea

• Extend QuickChick so it automatically relates checkers to Coq propositions that capture the conjecture under test.

• Manually prove these propositions equivalent to the desired high-level declarative specifications

Guarantee

If we could enumerate the output space of the generators used to by the checker without producing any counter examples then we would have a proof by exhaustion for the desired high-level specification
Strategy 1

- Map generators to sets of outcomes, i.e. the sets of values that have non-zero chance of being generated
  - Use logical predicates to represent sets
    - An element \( a : A \) belongs to a set that is represented by \( P : A \rightarrow \text{Prop} \) if and only if \( P \ a \)

- Map checkers to logical propositions using the sets of outcomes of the generators that they use
  - If a generator \( G \) for type \( A \) is mapped to \( S : A \rightarrow \text{Prop} \) then
    - \( \forall x, S \ x \rightarrow f \ x = \text{true} \)
Strategy II

• Use the sets of outcomes semantics of generators to prove:
  ♦ soundness
    ▶ All the values that are generated satisfy a certain predicate
  ♦ completeness
    ▶ All the values that satisfy a certain predicate can be generated
  ♦ correctness
    ▶ soundness + completeness

• Use the logical predicates obtained from checkers to prove that they correspond the desired declarative specification
Generators

- Generators are written using a library of combinators (e.g. bind, return, elements, frequency, ...)
  - *Primitive* combinators: they depend from the internal generator representation
  - *Non-primitive* combinators: they are built on top of other combinators

- *Overload* combinators with two kinds of semantics
  - actual generation semantics
  - sets of outcomes semantics

- Abstract from the generator representation: Make generators parametric in the generator type constructor
  - Instantiate them with the set representation to map them to sets of outcomes
  - or with the actual generator representation to generate data
Set Representation

\[
\text{Definition } \text{Pred} \ (A : \text{Type}) : \text{Type} := A \to \text{Prop}.
\]

\[
\text{Definition } \text{set_eq} \ \{A\} \ (m1 \ m2 : \text{Pred} \ A) := \forall A, \ m1 \ A \leftrightarrow m2 \ A.
\]

\[
\text{Infix } " \leftrightarrow " := \text{set_eq}.
\]

- Very compact set representation
  - Easily models infinite sets
  - Proof-oriented: facilitates reasoning for set membership
- Primitive combinators need to be implemented differently for each type constructor
Type classes to the rescue

Class \( \text{GenMonad} (M: \text{Type} \to \text{Type}) :=\)

\[
\begin{align*}
\text{bindGen: } & \forall \{A B: \text{Type}\}, \ M A \to (A \to M B) \to M B; \\
\text{returnGen: } & \forall \{A: \text{Type}\}, \ A \to M A; \\
\text{fmapGen: } & \forall \{A B: \text{Type}\}, \ (A \to B) \to M A \to M B; \\
\text{choose: } & \forall \{A: \text{Type}\} \ `(\text{Random A}, \ A \ast A) \to M A; \\
\text{sized: } & \forall \{A: \text{Type}\}, \ (\text{nat} \to M A) \to M A; \\
\text{suchThatMaybe: } & \forall \{A: \text{Type}\}, \ M A \to (A \to \text{bool}) \to \\
& \quad M (\text{option A});
\end{align*}
\]

- All the primitive combinators are included in the type class
- Both generator type constructors are instances of this type class
- The set of outcome definitions of the primitive combinators is \textbf{axiomatic}
- The methods of the type class are implicitly parameterized by
  the type constructor and the corresponding instance
Axioms

\[
\text{returnGen } a \equiv \{ x \mid x = a \}
\]

\[
\text{bindGen } G f \equiv \{ x \mid \exists g, G g \land f g x \} \leftarrow \bigcup_{g \in G} f g
\]

\[
\text{fmapGen } f G \equiv \{ x \mid \exists g, G g \land x = f g \}
\]

\[
\text{choose } (lo, hi) \equiv \{ x \mid lo \leq x \leq hi \}
\]

\[
\text{sized } f \equiv \{ x \mid \exists n, f n x \} \leftarrow \bigcup_{n \in \mathbb{N}} f n
\]

\[
\text{suchThatMaybe } g P \equiv \{ x \mid x = \text{None} \lor \\
\exists y, x = \text{Some } y \land g y \land P y \}
\]
Non-primitive combinators

- Non-primitive combinators are built on top of the interface provided by the type class.
- We move the definitions of non-primitive combinators inside a section in which we assume in context a type constructor which is instance of the `AbstractGen` type class.
  - No modification to their code is required.
- Primitive combinators used are automatically instantiated with the type constructor and the instance assumed in context.
Non-primitive combinators

Example

Section Utilities.

Context \{\text{Gen} : \text{Type} \to \text{Type}\}
\{H : \text{GenMonad Gen}\}.

Definition oneof \{\text{A} : \text{Type}\} (\text{def: Gen A}) (\text{gs : list (Gen A)})
: Gen A :=
bindGen (choose (0, length gs − 1)) (fun n ⇒
nth \text{def} \text{gs} n).

...  
...  

End Utilities.
Lemma Library for Non-primitive Combinators

- Using the sets of outcomes semantics we prove correctness for each non-primitive generator combinator
- These lemmas can be used in proofs about user defined generators that use the combinators
  - less proof duplication and reusability
  - independence from the implementation of combinators
  - compositional and more robust proofs
Lemma vectorOf_equiv:
\[ \forall \{A : \text{Type}\} \ (k : \text{nat}) \ (g : \text{Pred} \ A), \]
\[ \text{vectorOf} \ k \ g \ \leftrightarrow \ \text{fun} \ l \ \Rightarrow \ (\text{length} \ l = k \land \forall \ x, \text{In} \ x \ l \rightarrow g \ x). \]

Lemma listOf_equiv:
\[ \forall \{A : \text{Type}\} \ (g : \text{Pred} \ A), \]
\[ \text{listOf} \ g \ \leftrightarrow \ \text{fun} \ l \ \Rightarrow \ (\forall \ x, \text{In} \ x \ l \rightarrow g \ x). \]

Lemma elements_equiv:
\[ \forall \{A\} \ (l : \text{list} \ A) \ (\text{def} : A), \]
\[ (\text{elements} \ \text{def} \ l) \ \leftrightarrow \ (\text{fun} \ e \ \Rightarrow \ \text{In} \ e \ l \lor (l = \text{nil} \land e = \text{def})). \]

Lemma frequency_equiv:
\[ \forall \{A\} \ (l : \text{list} \ (\text{nat} \ast \text{Pred} \ A)) \ (\text{def} : \text{Pred} \ A), \]
\[ (\text{frequency} \ \text{def} \ l) \ \leftrightarrow \]
\[ \text{fun} \ e \ \Rightarrow \ (\exists \ (n : \text{nat}) \ (g : \text{Pred} \ A), \]
\[ \text{In} \ (n, \ g) \ l \land g \ e \land n <> 0) \lor \]
\[ ((l = \text{nil} \lor \forall \ x, \text{In} \ x \ l \rightarrow \text{fst} \ x = 0) \land \text{def} \ e). \]
Checkers

- Checkers are essentially generators of testing results
- We map them to a proposition that holds iff all the results that belong to the sets of outcomes are successful
  - The result of a test input is successful if it is equal with the expected
- The simplest form of checkers are boolean predicates
- More complex checkers can be written by utilizing property combinators
  - change the expected outcome, change default generators, instrumentation
  - We provide a library of correctness lemmas
Checkers

- Checkers are represented internally with the type operator `Property`.

```verbatim
Definition Property (Gen : Type → Type) := Gen QProp.
```

- We use the function `semProperty` to map them to logical propositions

```verbatim
Definition semProperty (P : Property Pred) : Prop :=
   ∀ qp, P qp → success qp = true.
```
Testable type class

- Testable type class provides a canonical way of turning types that can be tested into a Property
- Anything testable can be mapped to a proposition

```haskell
Class Testable {Gen : Type → Type} (A : Type) : Type :=
{
    property : A → Property Gen
}.

Definition semTestable {A : Type} {_: Testable A} (a : A) : Prop :=
    semProperty (property a).
```
forAll and implication Lemmas

Lemma semForAll:
\[ \forall \{A \text{ prop : Type}\} \{H1 : \text{Testable prop}\} \{H2 : \text{Show A}\} \ (\text{gen : Pred A}) \]
\[ (f : A \to \text{prop}), \]
\[ \text{semProperty \ (forall \ gen \ f) } \leftrightarrow \ \forall a : A, \ \text{gen a } \to \ \text{semTestable (f a)}. \]

Lemma semImplication:
\[ \forall \{\text{prop : Type}\} \{H : \text{Testable prop}\} \ (p : \text{prop}) \ (b : \text{bool}), \]
\[ \text{semProperty \ (b } \rightarrow \text{p) } \leftrightarrow \ b = \text{true } \rightarrow \ \text{semTestable p}. \]
Lemma Library for Checker Combinators II

Lemmas for specific testable types

Lemma semBool:
\[ \forall (b : \text{bool}), \; \text{semTestable } b \iff b = \text{true}. \]

Lemma semFun:
\[ \forall \{A \text{ prop : Type}\} \{H1 : \text{Show } A\} \{H2 : \text{Arbitrary } A\} \{H3 : \text{Testable } \text{prop}\}
\quad (f : A \to \text{prop}),
\quad \text{semTestable } f \iff \forall (a : A), \; \text{arbitrary } a \to \text{semTestable } (f \; a). \]

arbitrary here is a generator for elements of type A. It is a method of the Arbitrary type class that provides a common interface for generation. Testable type class use by default these generators to derive a Property.
Identity Lemmas

Some combinators do not affect the testing outcome. They are used for instrumentation purposes.

Lemma \textit{semCallback}\_id:
\[
\forall \{\text{prop : Type} \} \{\text{H : Testable prop} \} (\text{cb : Callback}) (\text{p : prop}),
\text{semProperty (callback}\ cb\ p) \leftrightarrow \text{semTestable p}.
\]

Lemma \textit{semWhenFail}\_id:
\[
\forall \{\text{prop : Type} \} \{\text{H : Testable prop} \} (\text{s : String.string}) (\text{p : prop}),
\text{semProperty (whenFail}\ s\ p) \leftrightarrow \text{semTestable p}.
\]

Lemma \textit{semPrintTestCase}\_id:
\[
\forall \{\text{prop: Type} \} \{\text{H : Testable prop} \} (\text{s: String.string}) (\text{p: prop}),
\text{semProperty (printTestCase}\ s\ p) \leftrightarrow \text{semTestable p}.
\]
Case Study
Red-black Trees
Red-Black Trees

- A self-balancing data structure
- Binary trees with an additional color label to each node

```
Inductive color := Red | Black.
Inductive tree :=
  | Leaf : tree
  | Node : color → tree → nat → tree → tree.
```

- The should preserve the following invariants
  ♦ The root is always black
  ♦ The leaves are empty and black
  ♦ For each node the path to each possible leaf has the same number of black nodes
  ♦ Red nodes can only have black children

- If the invariants are preserved then the longest path from the root is at most two times longer that the shortest
- The `insert` method should preserve the invariant
  ♦ We want to test that!
Red-Black Trees

- A self-balancing data structure
- Binary trees with an additional color label to each node

```
Inductive color := Red | Black.
Inductive tree :=
  | Leaf : tree
  | Node : color → tree → nat → tree → tree.
```

- The should preserve the following invariants
  - The root is always black
  - The leaves are empty and black
  - For each node the path to each possible leaf has the same number of black nodes
  - Red nodes can only have black children

- If the invariants are preserved then the longest path from the root is at most two times longer than the shortest
- The `insert` method should preserve the invariant
  - We want to test that!
The Red-Black Invariant

\[
\text{Inductive } \text{is\_redblack}: \text{tree} \to \text{color} \to \text{nat} \to \text{Prop} :=
\]

| \text{IsRB\_leaf}: \forall c, \ \text{is\_redblack Leaf} c \ 0 |
| \text{IsRB\_r}: \forall n \ tl \ tr \ h, |
| \hspace{1em} \text{is\_redblack tl Red} h \ \to \ \text{is\_redblack tr Red} h \ \to |
| \hspace{1em} \text{is\_redblack (Node Red tl n tr) Black} h |
| \text{IsRB\_b}: \forall c \ n \ tl \ tr \ h, |
| \hspace{1em} \text{is\_redblack tl Black} h \ \to \ \text{is\_redblack tr Black} h \ \to |
| \hspace{1em} \text{is\_redblack (Node Black tl n tr) c (S} h). |

- \text{is\_redblack } t \ c \ h \text{ means that } t \text{ is a subtree of a well-formed RB tree}
  - ♦ in \text{color-context} c \text{ (the color of the parent node)}
  - ♦ with \text{black-height} t \text{ (# black nodes in each path to a leaf)}

- A tree \( t \) satisfies the RB invariant iff:

\[
\exists h, \text{is\_redblack } t \ h \text{ Red}
\]
VeriQuickChick

System Under Test

Implementation
Executable Definitions

equivalence
proofs

Model
Declarative Definitions

VeriQuickChick

QuickChick

Property Checkers

Propositions

Predicates

equivalence
proofs

Propositions

Predicates

Generators

equivlence
proofs

Sets of outcomes
semantics

use
expression as

informal conjecture

trusts high-level specification

sets of outcomes
semantics
The Red-Black Invariant

- **insert** should preserve the invariant:

  \[
  \forall x \ t \ h, \ is\_redblack \ h \ Red \ t \rightarrow \\
  \exists h', \ is\_redblack \ h' \ Red \ (insert \ x \ t)
  \]

- In order to be able to test this we need
  - A decision procedure to determine whether a tree satisfies the RB invariant
  - A generator for RB trees
    - Should generate only trees that satisfy the invariant
    - Filtering out ill-formed RB trees is not an option
The Red-Black Invariant

• **insert** should preserve the invariant:

\[
\forall x \ t \ h, \ is\_redblack \ h \ Red \ t \rightarrow \\
\exists h', \ is\_redblack \ h' \ Red \ (insert \ x \ t)
\]

• In order to be able to test this we need
  ♦ A decision procedure to determine whether a tree satisfies the RB invariant
  ♦ A generator for RB trees
    ▶ Should generate only trees that satisfy the invariant
    ▶ Filtering out ill-formed RB trees is not an option
We need a decisional procedure to determine whether a tree satisfies the RB invariant.

```plaintext
Fixpoint is_redblack_dec (t : tree) (c: color): bool :=
    match t with
    | Leaf ⇒ true
    | Node c' tl _ tr ⇒
        match c' with
        | Black ⇒
            (black_height_dec tl == black_height_dec tr) &&
            is_redblack_dec tl Black && is_redblack_dec tr Black
        | Red ⇒
            match c with
            | Black ⇒
                (black_height_dec tl == black_height_dec tr) &&
                is_redblack_dec tl Red && is_redblack_dec tr Red
            | Red ⇒ false
        end
    end
end.
```
Executable Definitions

Does it correspond to the inductive definition? Yes!

```
Lemma is_redblack_exP:
  ∀ (t : tree) (c : color),
  reflect (exists n, is_redblack t c n) (is_redblack_dec t c).
```
Section Generators.

Context \{ Gen : Type \rightarrow Type \}
\{ H: \text{GenMonad Gen} \}.

Definition genColor := elements Red [Red; Black].

Fixpoint genRBTree_height (h : nat) (c : color) :=
  match h with
  | 0 ⇒
    match c with
      | Red ⇒ returnGen Leaf
      | Black ⇒ oneof (returnGen Leaf)
        [returnGen Leaf;
          bindGen arbitraryNat (fun n ⇒
            returnGen (Node Red Leaf n Leaf))]
    end
  | S h ⇒ ...
  end.

Definition genRBTree := sized (fun h ⇒ genRBTree_height h Red).

End Generators.
VeriQuickChick

System Under Test

- Implementation
  - Executable Definitions
    - equivalence
    - proofs
  - Model
    - Declarative Definitions

VeriQuickChick

QuickChick

- Property Checkers
  - Generators
    - use

- Propositions
  - Predicates
    - use
    - sets of outcomes
    - semantics
    - equivalence
    - proofs

- Specifications
  - Propositions
    - Predicates
      - equivalence
      - proofs
      - use
      - trusts high-level specification
Correctness for Red-black Tree Generator

We want to prove that the generator generates only trees that satisfy the RB invariant and also that it can generate all the possible trees that satisfy the RB invariant.

Lemma genRBTree_correct:
\[
\text{genRBTree} \iff (\text{fun } t \Rightarrow \exists h, \text{is_redblack } t \text{ Red } h).
\]

We need an intermediate lemma

Lemma genRBTree_height_correct:
\[
\forall c \ h, \\
(\text{genRBTree_height } h \ c) \iff (\text{fun } t \Rightarrow \text{is_redblack } t \ c \ h).
\]
System Under Test

Implementation
Executable Definitions

equivalence

proofs

Model
Declarative Definitions

VeriQuickChick

QuickChick

Property Checkers

Propositions

Predicates

Specifications

Propositions

Predicates

use

use

use

use

use

use

Informal Conjecture

trusts high-level specification

Sets of outcomes

semantics

expressed as
We can now write the checker for the property:

```coq
Section Checker.
  Context {Gen : Type → Type}
    {H: GenMonad Gen}.

  Definition insert_is_redblack_checker : Property Gen :=
    forAll arbitraryNat (fun n ⇒
      forAll genRBTree (fun t ⇒
        is_redblack_dec t Red ==> is_redblack_dec (insert n t) Red)).

End Checker.
```
Correctness for Checker

.. and prove that it indeed tests the right thing

\[
\text{Definition insert_is_redblack} := \\
\forall x \ s \ h, \ \text{is_redblack} s \ Red \ h \rightarrow \exists h', \ \text{is_redblack} (\text{insert} \ x \ s) \ Red \ h'.
\]

\[
\text{Lemma insert_is_redblack_checker_correct:} \\
\text{semProperty insert_is_redblack_checker} \leftrightarrow \text{insert_is_redblack}.
\]
System Under Test

Implementation
Executable Definitions

equivalence
proofs

Model
Declarative Definitions

VeriQuickChick

QuickChick

Property Checkers

Generators

semantics

sets of outcomes

semantics

use

Propositions

Predicates

use

equivalence
proofs

use

Specsifications

equivalence
proofs

use

informal conjecture

trusts high-level specification

expressed as
Conclusion

- We provide a mechanism to verify that a conjecture under test conforms to a high-level specification
- We facilitate reasoning for probabilistic programs
  - set of outcomes abstraction
- We proved high-level specifications about combinators
  - Proofs: 600 LOC
  - First step towards a fully verified PB testing framework
- We applied our methods to verify complex generators used to test an IFC machine
  - Generators: 350 LOC / Proofs: 900 LOC
  - ability to verify existing code
  - scalability
  - modularity
- Although reduced, manual effort is still required for the proofs
Future Work

- Remove the axioms by proving that the sets of outcomes of primitive combinators are indeed the those we assume
  - Fully verified PB testing framework
  - This would require deeper integration in Coq
    - Reasoning about random seed and generators of numeric and boolean values

- Verification of a framework for synthesizing generators from specifications
  - automation + formal guarantees

- Facilitate reasoning for the underlying probability distributions
  - instantiate generators with probability monad
Thank You!

Questions?
Record Result :=
  MkResult {
    ok : option bool; (* Testing outcome *)
    expect : bool; (* Expected outcome *)
    ... (* Other fields used for tracing *)
  }.

Inductive Rose (A : Type) : Type :=
  MkRose : A → Lazy (list (Rose A)) → Rose A.

Record QProp : Type := MkProp
{
  unProp : Rose Result
}.

Definition Property (Gen : Type → Type) := Gen QProp.
Definition resultSuccessful (r : Result) : bool :=
    match r with
        | MkResult (Some res) expected _ _ _ _ ⇒
            res == expected
        | _ ⇒ true
    end.

Definition success qp :=
    match qp with
        | MkProp (MkRose res _) ⇒ resultSuccessful res
    end.

Definition semProperty (P : Property Pred) : Prop :=
    ∀ qp, P qp → success qp = true.